roots of $F_g(X)$ are g, g^{p-1}, and g^{-p}. Then the method represents the powers of g using their trace over the field GF(p^2). The method then selects a private key. The method then computes a public key as a function of g and the private key. The public key can be used to encrypt a message and the public and private key can be used to decrypt the message. The public and private key can be used for signing a message and the public key can be used for verifying the signature. A Diffie-Hellman key exchange or other related scheme can be conducted using the public key generated by the method. The resulting invention reduces the bit-length of public keys and other messages, thereby reducing the bandwidth requirements of telecommunications devices, and reduces the computational effort required to encrypt/decrypt and to generate/verify digital signatures.

DELETE the current Abstract of the Disclosure and INSERT the following:

Efficient and Compact Subgroup Trace Representation ("XTR")

Abstract of the Disclosure

The invention is a method, system, computer program, computer program article of manufacture, and business method for providing improvements in key generation and cryptographic applications in public key cryptography, by both reducing: 1) the bit-length of public keys and other messages, thereby reducing the bandwidth requirements of telecommunications devices, such as wireless telephone sets, and 2) the computational effort required to generate keys, to encrypt/decrypt and to generate/verify digital signatures. The method of the invention determines a public key having a reduced length and a number p, using GF(p^2) arithmetic to achieve GF(p^6) security, without explicitly constructing GF(p^6).

IN THE CLAIMS

The Applicants respectfully request entry of this Amendment to **CANCEL** claims 1-24

and **ADD** claims 25-56.

Canceled Claims

Please **CANCEL** claims 1-24.

New Claims

25. (New) A method of determining a public key having an optionally reduced length and a number p, using GF(p) or GF(p^2) arithmetic to achieve GF(p^6) security, without explicitly constructing GF(p^6), comprising:

selecting a number q and a number p such that $p^2 - p + 1$ is an integer multiple of q;

selecting a number g of order q, where g and its conjugates can be represented by B, where $F_g(X) = X^3 - BX^2 + B^pX - 1$ and the roots are g, g^{p^2}, g^{-p}; and

representing the powers of the conjugates of g using their trace over the field GF(p^2).

26. (New) A method of generating a private key, and computing a public key as a function of p, q, and B generated by the method of claim 25, and the private key.

27. (New) A method of encrypting a message using the public key generated by the method of claim 26.

28. (New) A method of decrypting a message using the public key and the private key generated by the method of claim 26.

29. (New) A method of signing a message using the public key and the private key generated by the method of claim 26.

30. (New) A method of verifying a signature using the public key generated by the method of claim 26.

31. (New) A method of key exchange using the public key and the private key generated by the method of claim 26.

32. (New) A method of Diffie-Hellman key exchange and related schemes using p, q, and B as generated by the method of claim 25.

33. (New) A system for determining a public key having an optionally reduced length and a number p, using GF(p) or GF(p^2) arithmetic to achieve GF(p^6) security, without explicitly constructing GF(p^6), comprising:

a processor for selecting a number q and a number p such that $p^2 - p + 1$ is an integer multiple of q;

said processor selecting a number g of order q, where g and its conjugates can be represented by B, where $F_g(X) = X^3 - BX^2 + B^pX - 1$ and the roots are g, g^{p^1}, g^{-p}; and

said processor representing the powers of the conjugates of g using their trace over the field GF(p^2).

34. (New) A system of generating a private key, and computing a public key as a function of p, q, and B generated by the system of claim 33, and the private key.

35. (New) A system of encrypting a message using the public key generated by the system of claim 34.

36. (New) A system of decrypting a message using the public key and the private key generated by the system of claim 34.

37. (New) A system of signing a message using the public ken and the private key generated by the system of claim 34.

38. (New) A system of verifying a signature using the public key generated by the system of claim 34.

39. (New) A system of key exchange using the public key and the private key generated by the system of claim 34.

40. (New) A system of Diffie-Hellman key exchange and related schemes using p, q, and B as generated by the system of claim 33.

41. (New) A computer program article of manufacture, comprising:

a computer readable medium for determining a public key having an optionally reduced length and a number p, using GF(p) or GF(p^2) arithmetic to achieve GF(p^6) security, without explicitly constructing GF(p^6), comprising:

a computer program means in said computer readable medium, for selecting a number q and

a number p such that $p^2 - p + 1$ is an integer multiple of q;

a computer program means in said computer readable medium, for selecting a number g of order q, where g and its conjugates can be represented by B, where $F_g(X) = X^3 - BX^2 + B^pX - 1$ and the roots are g, g^{p^2}, g^{-p}; and

a computer program means in said computer readable medium, for representing the powers of the conjugates of g using their trace over the field GF(p^2).

42. (New) The article of manufacture of claim 41, which further comprises:

a computer program means in said computer readable medium, for generating a private key, and computing a public key as a function of p, q, and B, and the private key.

43. (New) The article of manufacture of claim 42, which further comprises:

a computer program means in said computer readable medium, for encrypting a message using the public key.

44. (New) The article of manufacture of claim 42, which further comprises:

a computer program means in said computer readable medium, for decrypting a message using the public key and the private key.

45. (New) The article of manufacture of claim 42, which further comprises:

a computer program means in said computer readable medium, for signing a message using the public key and the private key.

46. (New) The article of manufacture of claim 42, which further comprises:

a computer program means in said computer readable medium, for verifying a signature using the public key.

47. (New) The article of manufacture of claim 42, which further comprises:

a computer program means in said computer readable medium, for performing a key exchange using the public key and the private key.

48. (New) The article of manufacture of claim 41, which further comprises:

a computer program means in said computer readable medium, for performing a Diffie-Hellman key exchange or a related scheme using p, q, and B.

49. (New) A business method of determining a public key having an optionally reduced length and a number p, using GF(p) or GF(p^2) arithmetic to achieve GF(p^6) security, without explicitly constructing GF(p^6), comprising the steps of:

selecting a number q and a number p such that $p^2 - p + 1$ is an integer multiple of q;

selecting a number g of order q, where g and its conjugates can be represented by B, where $F_g(X) = X^3 - BX^2 + B^pX - 1$ and the roots are g, g^{p^2}, g^{-p}; and

representing the powers of the conjugates of g using their trace over the field GF(p^2).

50. (New) A method of generating a private key, and computing a public key as a function of p, q, and B generated by the business method of claim 49, and the private key.